Technology Management Group
Office of Information Services
Centers for Medicare & Medicaid Services

Procedure:

Request for Fire Call ID

September 2005

Document Number: CMS-TMG-PROC-INF06-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes the procedure for requesting a Fire Call ID for emergency access to secure automated systems operating in the production environment at the Centers for Medicare and Medicaid Services (CMS).

For security reasons, CMS does not allow system developers and system maintainers to have access authority or system privilege to make uncontrolled changes directly to automated systems operating in the production environment. Certain emergency situations, however, may necessitate bypassing the normal production change control procedure in order to effect an immediate change directly to an automated system operating in the production environment.

A Fire Call ID is an established logon user ID and password with special or powerful security access privileges, established to handle emergency situations. A Fire Call ID provides individuals, such as system maintainers, with controlled access to system data and files. In the event of a critical error or abnormal end, unprivileged users can gain access to correct emergency problems with automated systems in the production environment through the use of a Fire Call ID. To ensure a proper level of security, however, the issuance and use a Fire Call ID must be strictly controlled, monitored, and managed.

2. REFERENCES

- CMS Policy for the Information Security Program
- CMS Information Security Incident Handling Procedures

3. SCOPE

This procedure applies to all CMS software applications and automated systems operating within the production environment of the CMS Data Center in Woodlawn, Maryland.

4. ROLES AND RESPONSIBILITIES

The following entities have specific responsibilities related to the implementation of this procedure:

4.A. System Maintainer

For the purposes of this procedure, the System Maintainer is responsible for the following:

- Determining and justifying the need for use of the Fire Call ID to make a change(s) to an automated system or software application operating in the production environment at the CMS Data Center;

- Contacting the System Owner/Manager of the automated system/application to request the use of the Fire Call ID;
- Taking ownership of the Fire Call ID from the System Owner/Manager when it is issued;
- Being accountable for the activities performed using the Fire Call ID until its use is revoked; and
- Notifying the System Owner/Manager immediately when use of the Fire Call ID is completed.

4.B. System Owner/Manager

The System Owner/Manager is the individual on record at the CMS Data Center as the authorized point of contact for a specific automated system or software application operating in the CMS production environment. For the purposes of this procedure, the System Owner/Manager is responsible for the following:

- Ensuring that the CMS Data Center has a current telephone number at which the System Owner/Manager may be reached in the event of an emergency production situation;
- Contacting the CMS Data Center Shift Manager to request the issuance of the Fire Call ID, when an valid emergency situation occurs with an automated system or software application operating in the production environment, for which the System Owner/Manager is responsible;
- Providing the issued Fire Call ID to the System Maintainer for subsequent use; and
- Notifying the CMS Data Center Shift Manager immediately when the System Maintainer identifies that the use of the issued Fire Call ID has been completed.

4.C. Office of Information Services (OIS)/ Technology Management Group (TMG)

For the purposes of this procedure, the OIS/TMG On-Call Manager is responsible for overseeing the creation of the Fire Call ID and the management of the release of the Fire Call ID for a specific production incident.

The Resource Access Control Facility (RACF) Team of the Security Operations Staff in the OIS/TMG has the following responsibilities:

- Establishing and/or re-establishing the Fire Call logon user ID and password, and placing the Fire Call ID in a sealed envelope;
- Auditing all actions taken with the Fire Call ID;
- Requesting that the Consolidated IT Infrastructure Contract (CITIC) Contractor perform all necessary actions for securing the Fire Call ID within the CMS Data Center and for controlling and tracking the release of the Fire Call ID for specific requests; and
- Notifying the Supervisor of the System Owner/Manager who requested use of the Fire Call ID that the request and use occurred for the identified automated system/application.

4.D. Consolidated IT Infrastructure Contract (CITIC) Contractor

The CITIC Contractor is responsible for managing the CMS Data Center. As a result, the CITIC Contractor is responsible for securing, controlling, and tracking the release of the Fire Call ID.

The Fire Call ID must be secured in a designated, locked location of the CMS Data Center. Only the CMS Data Center Shift Manager shall have access to the Fire Call ID.

For the purposes of this procedure, the CMS Data Center Shift Manager is specifically responsible for the following:

- Calling the System Owner/ Manager that is on record for the identified automated system/application to verify that a Fire Call ID request is being initiated by the appropriate, authorized CMS employee;
- Issuing the Fire Call ID to the verified, requesting System Owner/Manager;
- Appropriately logging the issuance of a Fire Call ID in the CMS Fire Call ID Log;
- Sending an email notification to the OIS/TMG On-Call Manager and the "CMS CMSEUA" email resource to inform them when the Fire Call ID is issued;
- Sending an email notification to the OIS/TMG On-Call Manager and the "CMS CMSEUA" email resource to inform them that an issued Fire Call ID is to be revoked;
- Appropriately logging the date and time when an issued Fire Call ID has been revoked; and
- Securing the Fire Call ID received from the RACF Team of the Security Operations Staff of OIS/TMG in the designated, locked location of the CMS Data Center.

5. PROCEDURE

The following describes the sequence of steps that comprise the procedure for requesting and managing the issuance of the Fire Call ID:

- **STEP 1:** The System Maintainer determines the need for use of the Fire Call ID, and contacts the System Owner/Manager of the automated system/application that requires the emergency production change(s). The System Maintainer must provide justification for the emergency change(s), identifying why the change(s) cannot otherwise be made through the normal change control process. The System Maintainer must also provide an expected timeframe that the Fire Call ID will be needed.

- **STEP 2:** The System Owner/Manager calls the CMS Data Center Shift Manager to request issuance of the Fire Call ID. The System Owner/Manager must identify the automated system/application that is operating in production for which the Fire Call ID is needed, the reason for the Fire Call ID request, and the expected timeframe that the Fire Call ID will be needed.

- **STEP 3:** Using the telephone number maintained in the Call Back List within the CMS Data Center, the CMS Data Center Shift Manager attempts to call the System Owner/ Manager that is on record for the identified automated system/application to verify that the request is being initiated by the authorized CMS employee. If the call back is unsuccessful, the CMS Data Center Shift Manager reports the security incident in accordance with the established CMS Information Security Incident Handling Procedures, thereby ending any further processing of this Fire Call ID procedure.

- **STEP 4:** If the call back is successful, the CMS Data Center Shift Manager issues the Fire Call ID to the System Owner/Manager, and appropriately logs the transaction into the CMS Fire Call ID Log. The CMS Data Center Shift Manager also sends an email notification to the OIS/TMG On-Call Manager and the "CMS CMSEUA" email resource in Microsoft Outlook to report the Fire Call ID issuance transaction. The email notification must provide the name of the automated system/application and associated System Owner/Manager who received the Fire Call ID, the reason why the Fire Call ID was issued, the date and time the Fire Call ID was issued, and the expected timeframe that the Fire Call ID will be in use.

- **STEP 5:** The System Owner/Manager provides the Fire Call ID to the System Maintainer for use in applying the necessary emergency change(s) to the automated system/application in the production environment. When the change(s) are completed, the System Maintainer notifies the System Owner/Manager that the Fire Call ID is no longer needed, who in turn likewise notifies the CMS Data Center Shift Manager.

- **STEP 6:** The CMS Data Center Shift Manager sends an email notification to the OIS/TMG On-Call Manager and the "CMS CMSEUA" email resource in Microsoft Outlook to inform them that the Fire Call ID is no longer needed. The email sent to the "CMS CMSEUA" email resource will result in subsequent action by the RACF Team of the Security Operations Staff of OIS/TMG.

- **STEP 7:** The RACF Team of the Security Operations Staff of OIS/TMG revokes the current usage of the Fire Call ID, and creates a new password. The Fire Call logon user ID and new password are placed in a sealed envelope, which is then given to the CMS Data Center Shift Manager. The RACF Team of the Security Operations Staff also sends an email notification to the System Owner/Manager's Supervisor to inform the supervisor that the Fire Call ID request was initiated and completed for the identified automated system/application.

- **STEP 8:** The CMS Data Center Shift Manager places the envelope containing the Fire Call logon user ID and new password in the designated, secured location of the CMS Data Center for future use. The CMS Data Center Shift Manager also updates the CMS Fire Call ID Log to reflect the date and time that the previous Fire Call ID was revoked.

6. EFFECTIVE DATES

This procedure becomes effective on the date that the Director of OIS/TMG signs it, and remains in effect until officially superseded or cancelled by the OIS/TMG Director.

7. INFORMATION AND ASSISTANCE

For further information regarding this procedure, please contact the Director of the Security Operations Staff within the OIS/TMG.

8. APPROVED

/s/ 9/8/2005

Ronald Graham
Director, Technology Management Group

Date of Issuance

9. ATTACHMENTS

Form: CMS Fire Call ID Log

CMS FIRE CALL ID LOG

Automated System/ Application	System Owner/ Manager	Reason for FCID Use	Authorizing Data Center Manager	Date/Time FCID Issued	Expected Elapse Time for FCID Use	Date/Time FCID Revoked